EDUSUM

#1 Online Certification Guide

IBM C1000-162 STUDY GUIDE PDF

Grab the IBM Security QRadar SIEM Analysis Certification PDF Questions & Answers

Details of the Exam-Syllabus-Questions

C1000-162

IBM Certified Analyst - Security QRadar SIEM V7.5

64 Exam Questions – 64% Cut Score – Duration of 90 minutes

Table of Contents:

Get an Overview of the C1000-162 Certification:

Who should take the **C1000-162 exam**? This is the first question that comes to a candidate's mind when preparing for the Security QRadar SIEM Analysis certification. The C1000-162 certification is suitable for candidates who are keen to earn knowledge on the Security and grab their IBM Certified Analyst - Security QRadar SIEM V7.5. When it is about starting the preparation, most candidates get confused regarding the study materials and study approach. But C1000-162 study guide PDF is here to solve the problem. C1000-162 PDF combines some effective sample questions and offers valuable tips to pass the exam with ease.

Why Should You Earn the IBM C1000-162 Certification?

There are several reasons why one should grab the C1000-162 certification.

- The Security QRadar SIEM Analysis certification proves to be one of the most recognized certifications.
- The certification badge proves the knowledge of the candidate regarding subject matters and makes his resume presentable to potential candidates.
- Thus earning the IBM Certified Analyst - Security QRadar SIEM V7.5 is a powerful qualification for a prosperous career.

What is the IBM C1000-162 Security QRadar SIEM Analysis Certification Exam Structure?

Exam Name	IBM Certified Analyst - Security QRadar SIEM V7.5
Exam Code	C1000-162
Exam Price	$200 (USD)
Duration	90 mins
Number of Questions	64
Passing Score	64%
Books / Training	**IBM Certified Analyst: Security QRadar SIEM V7.5 - Exam C1000-162 Preparation Guide** **QRadar SIEM Analyst learning plan**
Schedule Exam	**Pearson VUE**
Sample Questions	**IBM Security QRadar SIEM Analysis Sample Questions**
Practice Exam	**IBM C1000-162 Certification Practice Exam**

Enhance Knowledge with C1000-162 Sample Questions:

Question: 1

What are events called when they are classified in the proper log source?

a) Stored events
b) Parsed events
c) Payload events
d) Unknown events

Answer: b

Question: 2

In QRadar, where is a list of offenses displaying associated source IP addresses?

a) Offense Summary > By Source IP
b) Offense Summary > New Search > Advanced Search
c) Log Activity > Offense Source Summary > Offenses
d) Log Activity > Add Filter > Source IP > offense_assigned

Answer: a

Question: 3

Which report can you run to find rules or building blocks that use performance-intensive tests that are not at the end of the test list?

a) CRE report
b) R2R report
c) Active Rules report
d) Tuning Finding report

Answer: d

Question: 4

How can a QRadar analyst identify the gap between the rules deployed on QRadar and rules needed to cover the security use cases?

a) Use the QRadar Assistant app
b) Use the Offense tab to add new rules
c) Use the IBM X-Force Exchange portal
d) Use the content extension filters on Use Case Manager app

Answer: d

Question: 5

An analyst is investigating rules that are deployed in the QRadar deployment. Where does the analyst determine which rules are most active in generating offenses?

a) In the Offenses tab, on the All Offenses menu, checking the Flows column
b) In the Offenses tab, on the My Offenses menu, checking the Events column
c) In the Offenses tab, on the Rules menu, checking the Offense Count column
d) In the Offenses tab, on the Rules menu, checking the Events/Flow Count column

Answer: c

Question: 6

Offense chaining is possible based on which parameter?

a) Rule type
b) Rule response
c) Offense index field
d) Rule response limiter

Answer: c

Question: 7

Based on which factors will the magistrate prioritize the offenses and assign the magnitude values?

a) Relevance, severity, and risk
b) Severity, relevance, and credibility
c) Risk, severity, and number of events
d) Credibility, priority, and number of events

Answer: b

Question: 8

Which two (2) of these categories can be used for Ariel Query Language?

a) Assets
b) Widget
c) Network
d) Keyword
e) Database

Answer: d, e

Question: 9

When a QRadar QFlow Collector is combined with QRadar and flow processors, what is the highest OSI layer visible in Network Activity?

a) Layer 7
b) Layer 5
c) Layer 4
d) Layer 1

Answer: a

Question: 10

What are the key elements used by the Report wizard in QRadar to create a report?

a) Font, color, and size
b) Content, style, and design
c) Layout, container, and content
d) Schedule, generate, and export

Answer: c

What Study Guide Works Best in acing the IBM C1000-162 Security QRadar SIEM Analysis Certification?

The C1000-162 study guide is a combination of some proven study tips and the combination of all valuable study materials like sample questions, syllabus and practice tests in one place.

Explore the Syllabus Topics and Learn from the Core:

If you are determined to earn success in the Security QRadar SIEM Analysis exam, getting in full touch of the **syllabus** is mandatory. During preparation, you might not like all syllabus sections or topics, but try to get at least the fundamental knowledge from the sections you don't like. The more you possess knowledge on all syllabus sections, the more is the chance to attempt maximum number of questions during the actual exam.

Make Your Schedule:

Studying and completing the syllabus becomes easier, if you work on the syllabus topics after making a schedule. Your syllabus must mention what areas you want to cover and within what time. Once you make a schedule and follow it regularly, syllabus completion becomes easier and preparation becomes smoother.

Get Expert Advice from the Training:

Do not forget to join the IBM C1000-162 training if it is providing any. Training enhances the practical knowledge of a candidate, which helps them to work well in the practical field during projects.

Get Access to the PDF Sample Questions:

If your study material is in a PDF format or the materials are mobile-friendly, what could be better than that? Get access to the free sample questions and keep enhancing your knowledge beyond the syllabus.

Avoid Dumps and utilize the IBM C1000-162 Practice Test:

Why should you rely on practice tests? The reason is simple: you must get familiar with the exam pattern before reaching the exam hall. An aspirant aware of the exam structure and time management during the exam preparation can perform well in the actual exam and attempt the maximum number of questions during the exam.

Many aspirants prefer to read from dumps, but they miss out on the self assessment method. Therefore, C1000-162 practice tests always stand out to be the better choice than dumps PDF.

Avail the Proven C1000-162 Practice Test for Success!!!

Do you want to pass the C1000-162 exam on your first attempt? Stop worrying; we, EduSum.com are here to provide you the best experience during your IBM Security QRadar SIEM V7.5 Analysis preparation. Try out our free mock tests to get a glimpse of our quality study materials, and build your confidence with the premium **C1000-162 practice tests**. Our expert-designed questions help you to improve performance and pass the exam on your first attempt.